

# ON THE INTEGRAL REPRESENTATION OF BINARY QUADRATIC FORMS AND THE ARTIN CONDITION

CHANG LV

**ABSTRACT.** For diophantine equations of the form  $ax^2 + bxy + cy^2 + g = 0$  over  $\mathbb{Z}$  whose coefficients satisfy some hypotheses, we show that the Artin condition is the only obstruction to the local-global principle for integral solutions of the equation. Some concrete examples are presented.

## 1. INTRODUCTION

The main theorem of a book by David A. Cox [1] is a beautiful criterion of the solvability of the diophantine equation  $p = x^2 + ny^2$ . The specific statement is

**Theorem.** Let  $n$  be positive integer. Then there is a monic irreducible polynomial  $f_n(x) \in \mathbb{Z}[x]$  of degree  $h(-4n)$  such that if an odd prime  $p$  divides neither  $n$  nor the discriminant of  $f_n(x)$ , then  $p = x^2 + ny^2$  is solvable over  $\mathbb{Z}$  if and only if  $\left(\frac{-n}{p}\right) = 1$  and  $f_n(x) = 0$  is solvable over  $\mathbb{Z}/p\mathbb{Z}$ . Here  $h(-4n)$  is the class number of primitive positive definite binary forms of discriminant  $-4n$ . Furthermore,  $f_n(x)$  may be taken to be the minimal polynomial of a real algebraic integer  $\alpha$  for which  $L = K(\alpha)$  is the ring class field of the order  $\mathbb{Z}[\sqrt{-n}]$  in the imaginary quadratic field  $K = \mathbb{Q}(\sqrt{-n})$ .

There are some generalizations considering the problem over quadratic fields.

By using classical results in the class field theory, the author and Yingpu Deng [3] gave the criterion of the integral solvability of the equation  $p = x^2 + ny^2$  for some  $n$  over a class of imaginary quadratic fields, where  $p$  is a prime element.

Recently, Harari [2] showed that the Brauer-Manin obstruction is the only obstruction for the existence of integral points of a scheme over the ring of integers of a number field, whose generic fiber is a principal homogeneous space (torsor) of a torus. After then Dasheng Wei and Fei Xu gave another proof in [9, 10] where the Brouer-Manin obstruction is constructive. This can be used to determine the existence of integral points for the scheme. In [9, Section 3] Wei also showed how to apply this method to binary quadratic diophantine equations. However, the so called **X**-admissible subgroup in [9] is not constructive, which lead to the difficulty for calculating an explicit criterion of the solvability.

Later Dasheng Wei [7] applied the method in [9] to give some criteria of the solvability of the diophantine equation  $x^2 - dy^2 = a$  over  $\mathbb{Z}$  for some  $d$ , by giving the specific **X**-admissible subgroup. He also determine which integers can be written as a sum of two integral squares for some of the quadratic fields  $\mathbb{Q}(\sqrt{\pm p})$  (in [6]),  $\mathbb{Q}(\sqrt{-2p})$  (in [8]) and so on.

---

*Date:* October 19, 2015.

*2000 Mathematics Subject Classification.* Primary 11D09, 11E12, 11D57; Secondary 11D57, 14L30, 11R37.

*Key words and phrases.* binary quadratic forms, integral points, ring class field.

In this article, we apply the method in [9] to diophantine equations of the form  $ax^2 + bxy + cy^2 + g = 0$  over  $\mathbb{Z}$ , a binary quadratic form representing an integer. By some additional hypotheses, we give the  $\mathbf{X}$ -admissible subgroup for the equation, from which we obtain criteria of the solvability in a more explicit way. This is more specific than what Wei did in [9, Section 3].

In Section 2, we introduce from [9] notations and the general result we mainly use in this paper, but in a modified way which focus on our goal. Then we give our results on the equation  $ax^2 + bxy + cy^2 + g = 0$  in Section 3. If the discriminant  $d$  is positive we need no additional hypothesis. But if  $d$  is negative, we add some hypotheses on it. The results state that the integral local condition together with the Artin condition completely describe the global integral solvability. We also give some examples showing the explicit criteria of the solvability.

## 2. SOLVABILITY BY THE ARTIN CONDITION

**2.1. Notations.** Let  $F$  be a number field,  $\mathfrak{o}_F$  the ring of integers of  $F$ ,  $\Omega_F$  the set of all places in  $F$  and  $\infty_F$  the set of all infinite places in  $F$ . Let  $F_{\mathfrak{p}}$  be the completion of  $F$  at  $\mathfrak{p}$  and  $\mathfrak{o}_{F_{\mathfrak{p}}}$  be the valuation ring of  $F_{\mathfrak{p}}$  for each  $\mathfrak{p} \in \Omega_F \setminus \infty_F$ . We also write  $\mathfrak{o}_{F_{\mathfrak{p}}} = F_{\mathfrak{p}}$  for  $\mathfrak{p} \in \infty_F$ . The adèle ring (resp. idele group) of  $F$  is denoted by  $\mathbb{A}_F$  (resp.  $\mathbb{I}_F$ ).

Let  $a, b, c$  and  $g$  be elements in  $\mathfrak{o}_F$  and suppose that  $-d = b^2 - 4ac$  is not a square in  $F$ . Let  $E = F(\sqrt{-d})$  and  $\mathbf{X} = \mathbf{Spec}(\mathfrak{o}_F[x, y]/(ax^2 + bxy + cy^2 + g))$  be the affine scheme defined by the equation  $ax^2 + bxy + cy^2 + g = 0$  over  $\mathfrak{o}_F$ . The equation

$$(2.1) \quad ax^2 + bxy + cy^2 + g = 0$$

is solvable over  $\mathfrak{o}_F$  if and only if  $\mathbf{X}(\mathfrak{o}_F) \neq \emptyset$ .

It is easy to see that (2.1) is equivalent to

$$(2.2) \quad \tilde{x}^2 + d\tilde{y}^2 = n,$$

where

$$\tilde{x} := 2ax + by,$$

$$\tilde{y} := y,$$

$$n := -4ag.$$

Denote  $R_{E/F}(\mathbb{G}_m)$  the Weil restriction (see [4]) of  $\mathbb{G}_{m,E}$  to  $F$ . Let

$$\varphi : R_{E/F}(\mathbb{G}_m) \longrightarrow \mathbb{G}_m$$

be the homomorphism of algebraic groups which represents

$$x \mapsto N_{E/F}(x) : (E \otimes_F A)^{\times} \longrightarrow A^{\times}$$

for any  $F$ -algebra  $A$ . Define the torus  $\mathbf{T} := \ker \varphi$ . Let  $\mathbf{X}_F$  be the generic fiber of  $\mathbf{X}$ . Then  $\mathbf{X}_F$  is naturally a  $\mathbf{T}$ -torsor by the action:

$$\begin{aligned} \mathbf{T}(A) \times \mathbf{X}_F(A) &\longrightarrow \mathbf{X}_F(A) \\ (u + \sqrt{-d}v, \tilde{x} + \sqrt{-d}\tilde{y}) &\mapsto (u + \sqrt{-d}v)(\tilde{x} + \sqrt{-d}\tilde{y}). \end{aligned}$$

One can check that

$$(2.3) \quad \mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}}) \subseteq \mathbf{Stab}(\mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})) := \{g \in \mathbf{T}(F_{\mathfrak{p}}) \mid g\mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}}) = \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})\}.$$

Denote by  $\lambda$  the embedding of  $\mathbf{T}$  into  $R_{E/F}(\mathbb{G}_m)$ . Clearly  $\lambda$  induces a natural injective group homomorphism

$$\lambda_E : \mathbf{T}(\mathbb{A}_F) \longrightarrow \mathbb{I}_E.$$

Let  $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-d}$  in  $E$  and  $L_{\mathfrak{p}} = L \otimes_{\mathfrak{o}_F} \mathfrak{o}_{F_{\mathfrak{p}}}$  in  $E_{\mathfrak{p}} = E \otimes_F F_{\mathfrak{p}}$ . Then

$$\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}}) = \{ \beta \in L_{\mathfrak{p}}^{\times} \mid N_{E_{\mathfrak{p}}/F_{\mathfrak{p}}}(\beta) = 1 \},$$

It follows that  $\lambda_E(\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})) \subseteq L_{\mathfrak{p}}^{\times}$ . Note that  $\lambda_E(\mathbf{T}(F)) \subseteq E^{\times}$  in  $\mathbb{I}_E$ . Let  $\Xi_L := \prod_{\mathfrak{p} \in \Omega_F} L_{\mathfrak{p}}^{\times}$  which is an open subgroup of  $\mathbb{I}_E$ . Then the following map induced by  $\lambda_E$  is well-defined:

$$\tilde{\lambda}_E : \mathbf{T}(\mathbb{A}_F)/\mathbf{T}(F) \prod_{\mathfrak{p} \in \Omega_F} \mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}}) \longrightarrow \mathbb{I}_E/E^{\times} \prod_{\mathfrak{p} \in \Omega_F} L_{\mathfrak{p}}^{\times}.$$

Now we assume that

$$(2.4) \quad \mathbf{X}(F) \neq \emptyset,$$

i.e.  $\mathbf{X}_F$  is a trivial  $\mathbf{T}$ -torsor. Fixing a rational point  $P \in \mathbf{X}(F)$ , for any  $F$ -algebra, we have an isomorphism

$$\begin{aligned} \phi_P : \mathbf{X}_F(A) &\cong \mathbf{T}(A) \\ x &\mapsto P^{-1}x \end{aligned}$$

induced by  $P$ . Since we can view  $\prod_{\mathfrak{p} \in \Omega_F} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$  as a subset of  $\mathbf{X}_F(\mathbb{A}_F)$ , the composition  $f_E := \lambda_E \phi_P : \prod_{\mathfrak{p}} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}}) \longrightarrow \mathbb{I}_E$  makes sense, mapping  $x$  to  $P^{-1}x$  in  $\mathbb{I}_E$ . Note that  $P$  is in  $E^{\times} \subset \mathbb{I}_E$  since it is a rational point over  $F$ . It follows that we can define the map  $\tilde{f}_E$  to be the composition

$$\prod_{\mathfrak{p}} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}}) \xrightarrow{f_E} \mathbb{I}_E \xrightarrow{\times P} \mathbb{I}_E$$

$$x \longmapsto P^{-1}x \longmapsto x.$$

It can be seen that the restriction to  $\mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$  of  $\tilde{f}_E$  is defined by

$$(2.5) \quad \tilde{f}_E[(x_{\mathfrak{p}}, y_{\mathfrak{p}})] = \begin{cases} (\tilde{x}_{\mathfrak{p}} + \sqrt{-d}\tilde{y}_{\mathfrak{p}}, \tilde{x}_{\mathfrak{p}} - \sqrt{-d}\tilde{y}_{\mathfrak{p}}) \in E_{\mathfrak{P}_1} \otimes E_{\mathfrak{P}_2} & \text{if } \mathfrak{p} \text{ splits in } E/F, \\ \tilde{x}_{\mathfrak{p}} + \sqrt{-d}\tilde{y}_{\mathfrak{p}} \in E_{\mathfrak{P}} & \text{otherwise,} \end{cases}$$

where  $\mathfrak{P}_1$  and  $\mathfrak{P}_2$  (resp.  $\mathfrak{P}$ ) are places of  $E$  above  $\mathfrak{p}$ .

Recall that  $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-d}$ ,  $L_{\mathfrak{p}} = L \otimes_{\mathfrak{o}_F} \mathfrak{o}_{F_{\mathfrak{p}}}$  and  $\Xi_L = \prod_{\mathfrak{p}} L_{\mathfrak{p}}^{\times}$  is an open subgroup of  $\mathbb{I}_E$ . By the *ring class field corresponding to  $L$*  we mean the class field  $H_L$  corresponding to  $\Xi_L$  under the class field theory, such that the Artin map gives the isomorphism  $\psi_{H_L/E} : \mathbb{I}_E/E^{\times}\Xi_L \cong \text{Gal}(H_L/E)$ . For any  $\prod_{\mathfrak{p} \in \Omega_F} (x_{\mathfrak{p}}, y_{\mathfrak{p}}) \in \prod_{\mathfrak{p} \in \Omega_F} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$ , noting that  $P$  is in  $E$ , we have

$$(2.6) \quad \psi_{H_L/E}(f_E(\prod_{\mathfrak{p}} (x_{\mathfrak{p}}, y_{\mathfrak{p}}))) = 1 \text{ if and only if } \psi_{H_L/E}(\tilde{f}_E(\prod_{\mathfrak{p}} (x_{\mathfrak{p}}, y_{\mathfrak{p}}))) = 1.$$

*Remark 2.7.* If  $\prod_{\mathfrak{p} \in \Omega_F} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}}) \neq \emptyset$ , then the assumption (2.4) we made before, that is  $\mathbf{X}(F) \neq \emptyset$ , holds automatically by the Hasse-Minkowski theorem on quadratic equations. Hence We can pick an  $F$ -point  $P$  of  $\mathbf{X}$  and obtain  $\phi_P$ .

**2.2. General results.** With above settings, Wei and Xu [9] obtained the following result on the solvability:

**Theorem 2.8** ([9] Corollary 1.6). Let  $\Xi \subseteq \mathbb{I}_E$  be an open subgroup such that the map

$$(2.9) \quad \hat{\lambda}_E : \mathbf{T}(\mathbb{A}_F)/\mathbf{T}(F)\mathbf{Stab}_{\mathbb{A}}(\mathbf{X}) \longrightarrow \mathbb{I}_E/E^\times \Xi$$

induced by  $\lambda_E$  is well defined and injective, where

$$\mathbf{Stab}_{\mathbb{A}}(\mathbf{X}) := \mathbf{T}(\mathbb{A}_F) \cap \prod_{\mathfrak{p}} \mathbf{Stab}(\mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})).$$

Let the abelian extension corresponding to  $\Xi$  and the Artin map be  $K_{\Xi}$  and  $\psi_{K_{\Xi}/E} : \mathbb{I}_E/E^\times \Xi_L \cong \text{Gal}(K_{\Xi}/E)$ , respectively. Then  $\mathbf{X}(\mathfrak{o}_F) \neq \emptyset$  if and only if there exists

$$\prod_{\mathfrak{p} \in \Omega_F} (x_{\mathfrak{p}}, y_{\mathfrak{p}}) \in \prod_{\mathfrak{p} \in \Omega_F} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$$

such that

$$\psi_{K_{\Xi}/E}(f_E(\prod_{\mathfrak{p}} (x_{\mathfrak{p}}, y_{\mathfrak{p}}))) = 1.$$

In fact, the original statement in [9] is more general: one allows  $\mathbf{X}$  to be any separated  $\mathfrak{o}_F$ -scheme of finite type whose generic fiber  $\mathbf{X}_F$  is a principal homogeneous space of  $\mathbf{T}$  and the extension  $E/F$  could be replaced by multiple ones, i.e., they are finite extensions  $E_1, E_2, \dots, E_m$  of  $F$ . Such an open subgroup  $\Xi$  making (2.9) injective is called an  $\mathbf{X}$ -admissible subgroup. However, when applied to quadratic equations, the subgroup is not constructive in [9], which lead to the difficulty for calculating an explicit criterion of the solvability.

In the previous section, we choose the subgroup to be  $\Xi_L = \prod_{\mathfrak{p}} L_{\mathfrak{p}}^\times$  where  $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-d}$  and  $L_{\mathfrak{p}} = L \otimes_{\mathfrak{o}_F} \mathfrak{o}_{F_{\mathfrak{p}}}$ . By some additional hypotheses, we prove that  $\Xi_L$  can be viewed as an admissible subgroup for  $\mathbf{X} = \mathbf{Spec}(\mathfrak{o}_F[x, y]/(ax^2 + bxy + cy^2 + g))$ . As a result, we can obtain criteria of the solvability in a more explicit way.

We will prove the following proposition mainly used in this paper, which is a Corollary to Theorem 2.8 (i.e. [9, Corollary 1.6]).

**Proposition 2.10.** *Let symbols be as before. Let  $u_1, u_2, \dots, u_r$  be elements that generate  $\mathfrak{o}_F^\times$ . Suppose for every integer set  $\{i_i\}_{i=1}^s$ , where  $s > 0$  and  $0 < i_1, i_2, \dots, i_s \leq r$ , the equation  $x^2 + dy^2 = u_{i_1}u_{i_2} \dots u_{i_s}$  is solvable over  $\mathfrak{o}_F$  or is not solvable over  $\mathfrak{o}_{F_{\mathfrak{p}}}$  for some place  $\mathfrak{p}$ . Then  $\mathbf{X}(\mathfrak{o}_F) \neq \emptyset$  if and only if there exists*

$$\prod_{\mathfrak{p} \in \Omega_F} (x_{\mathfrak{p}}, y_{\mathfrak{p}}) \in \prod_{\mathfrak{p} \in \Omega_F} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$$

such that

$$(2.11) \quad \psi_{H_L/E}(\tilde{f}_E(\prod_{\mathfrak{p}} (x_{\mathfrak{p}}, y_{\mathfrak{p}}))) = 1.$$

For the proof, we start with the following lemma to show that  $\Xi_L$  can be viewed as an admissible subgroup for  $\mathbf{X} = \mathbf{Spec}(\mathfrak{o}_F[x, y]/(ax^2 + bxy + cy^2 + g))$ .

**Lemma 2.12.** *Let  $u_1, u_2, \dots, u_r$  be elements that generate  $\mathfrak{o}_F^\times$ . Then the map  $\tilde{\lambda}_E$  is injective if for every integer set  $\{i_i\}_{i=1}^s$ , where  $s > 0$  and  $0 < i_1, i_2, \dots, i_s \leq r$ , the equation  $x^2 + dy^2 = u_{i_1}u_{i_2} \dots u_{i_s}$  is solvable over  $\mathfrak{o}_F$  or is not solvable over  $\mathfrak{o}_{F_{\mathfrak{p}}}$  for some place  $\mathfrak{p}$ .*

*Proof.* Recall that  $\mathbf{T} = \ker(R_{E/F}(\mathbb{G}_m) \longrightarrow \mathbb{G}_m)$ . Therefore we have

$$\mathbf{T}(F) = \{ \beta \in E^\times \mid N_{E/F}(\beta) = 1 \}$$

and

$$\mathbf{T}(\mathfrak{o}_{F_p}) = \{ \beta \in L_p^\times \mid N_{E_p/F_p}(\beta) = 1 \}.$$

Suppose  $t \in \mathbf{T}(\mathbb{A}_F)$  such that  $\tilde{\lambda}_E(t) = 1$ . Write  $t = \beta i$  with  $\beta \in E^\times$  and  $i \in \prod_p L_p^\times$ . Since  $t \in \mathbf{T}(\mathbb{A}_F)$  we have

$$N_{E/F}(\beta)N_{E/F}(i) = N_{E/F}(\beta i) = 1.$$

It follows that

$$N_{E/F}(i) = N_{E/F}(\beta^{-1}) \in F^\times \cap \prod_p \mathfrak{o}_{F_p}^\times = \mathfrak{o}_F^\times.$$

Suppose  $N_{E/F}(i) = u_{i_1}^{v_1} u_{i_2}^{v_2} \dots u_{i_s}^{v_s}$  where  $0 < i_1, i_2, \dots, i_s \leq r$  and  $v_i \in \mathbb{Z}$ . We can assume, without loss of generality, that  $v_1 = 2k_1, \dots, v_m = 2k_m$  are even and  $v_{m+1} = 2k_{m+1} - 1, \dots, v_s = 2k_s - 1$  are odd, where  $0 \leq m \leq s$ . Then

$$(2.13) \quad N_{E/F}(i u_{i_1}^{-k_1} \dots u_{i_s}^{-k_s}) = (u_{i_{m+1}} \dots u_{i_s})^{-1}.$$

If  $m = s$  then  $N_{E/F}(i u_{i_1}^{-k_1} \dots u_{i_s}^{-k_s}) = N_{E/F}(\beta u_{i_1}^{k_1} \dots u_{i_s}^{k_s}) = 1$ . Hence  $\beta u_{i_1}^{k_1} \dots u_{i_s}^{k_s} \in \mathbf{T}(F)$  and  $i u_{i_1}^{-k_1} \dots u_{i_s}^{-k_s} \in \prod_p \mathbf{T}(\mathfrak{o}_{F_p})$ . It follows that

$$u = \beta i = (\beta u_{i_1}^{k_1} \dots u_{i_s}^{k_s})(i u_{i_1}^{-k_1} \dots u_{i_s}^{-k_s}) \in \mathbf{T}(F) \prod_p \mathbf{T}(\mathfrak{o}_{F_p}).$$

Otherwise we know from (2.13) that the equation  $x^2 + dy^2 = (u_{i_{m+1}} \dots u_{i_s})^{-1}$  is solvable over  $\mathfrak{o}_{F_p}$  for every place  $p$  of  $F$ . Since  $u_{i_{m+1}} \dots u_{i_s} \in \mathfrak{o}_F$ , this is also true for the equation  $x^2 + dy^2 = u_{i_{m+1}} \dots u_{i_s}$ . By the hypothesis we know that  $x^2 + dy^2 = u_{i_{m+1}} \dots u_{i_s}$  is solvable over  $\mathfrak{o}_F$ . Let  $(x_0, y_0) \in \mathfrak{o}_F^2$  be such a solution and let

$$\begin{aligned} \zeta &= x_0 + y_0 \sqrt{-d}, \\ \gamma &= \beta u_{i_1}^{k_1} \dots u_{i_s}^{k_s} \zeta^{-1} \\ \text{and } j &= i u_{i_1}^{-k_1} \dots u_{i_s}^{-k_s} \zeta. \end{aligned}$$

Then  $N_{E/F}(\gamma) = N_{E/F}(j) = 1$ . Hence  $\gamma \in \mathbf{T}(F)$  and  $j \in \prod_p \mathbf{T}(\mathfrak{o}_{F_p})$ . It follows that  $u = \beta i = \gamma j \in \mathbf{T}(F) \prod_p \mathbf{T}(\mathfrak{o}_{F_p})$ . This finishes the proof.  $\square$

Now we are almost done in proving the proposition:

*Proof of the Proposition 2.10.* By the hypothesis we know from Lemma 2.12, that

$$(2.14) \quad \tilde{\lambda}_E : \mathbf{T}(\mathbb{A}_F)/\mathbf{T}(F) \prod_p \mathbf{T}(\mathfrak{o}_{F_p}) \longrightarrow \mathbb{L}_E/E^\times \prod_p L_p^\times$$

is injective. Since by (2.3) we have  $\prod_p \mathbf{T}(\mathfrak{o}_{F_p}) \subseteq \prod_p \mathbf{Stab}(\mathbf{X}(\mathfrak{o}_{F_p})) \subseteq \mathbf{Stab}_{\mathbb{A}}(\mathbf{X})$ . The statement of [9, Corollary 1.6] is also valid if we replace  $\mathbf{Stab}_{\mathbb{A}}(\mathbf{X})$  by a subgroup of it. In our case the subgroup is  $\prod_p \mathbf{T}(\mathfrak{o}_{F_p})$ . Hence we still call  $\Xi = \prod_p L_p^\times$  an  $\mathbf{X}$ -admissible subgroup. Then [9, Corollary 1.6] and the fact (2.6) give the result. For completeness, we give the argument below.

If  $\mathbf{X}(\mathfrak{o}_F) \neq \emptyset$ , then

$$\tilde{f}_E \left( \prod_p \mathbf{X}(\mathfrak{o}_{F_p}) \right) \cap E^\times \prod_p L_p^\times \supseteq \tilde{f}_E(\mathbf{X}(\mathfrak{o}_F)) \cap E^\times \neq \emptyset$$

Hence there exists  $x \in \prod_{\mathfrak{p} \in \Omega_F} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$  such that  $\psi_{H_L/E} \tilde{f}_E(x) = 1$ .

Conversely, suppose there exists  $x \in \prod_{\mathfrak{p}} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}})$  such that  $\psi_{H_L/E} \tilde{f}_E(x) = 1$  (here  $\tilde{f}_E$  makes sense by Remark 2.7), i.e.  $\lambda_E \phi_P(x) = f_E(x) \in \Xi_L = E^\times \prod_{\mathfrak{p}} L_{\mathfrak{p}}^\times$ . Since  $\tilde{\lambda}_E$ , i.e. (2.14), is injective, there are  $\tau \in \mathbf{T}(F)$  and  $\sigma \in \prod_{\mathfrak{p}} \mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})$  such that  $\tau\sigma = \phi_P(x) = P^{-1}x$ , i.e.  $\tau\sigma(P) = x$ . Since  $P \in \mathbf{X}(F)$  and  $\prod_{\mathfrak{p}} \mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}}) \subseteq \mathbf{Stab}_{\mathbb{A}}(\mathbf{X})$ , it follows that

$$\tau(P) = \sigma^{-1}(x) \in \mathbf{X}(F) \cap \prod_{\mathfrak{p}} \mathbf{X}(\mathfrak{o}_{F_{\mathfrak{p}}}) = \mathbf{X}(\mathfrak{o}_F).$$

Then the proof is done.  $\square$

The condition (2.11) is called the *Artin condition* in, for example, Wei's [7, 6, 8]. It interprets the fact that the Brauer-Manin obstruction is the only obstruction for existence of the integral points by conditions in terms of the class field theory. Consequently, assuming that the hypothesis in the proposition holds, the integral local condition together with the Artin condition completely describe the global integral solvability. As a result, in cases where the ring class fields are known it is possible to calculate the Artin condition, giving explicit criteria for the solvability.

### 3. THE INTEGRAL REPRESENTATION OF BINARY QUADRATIC FORMS OVER $\mathbb{Z}$

Now we consider the case where  $F = \mathbb{Q}$  which is our focus. We now distinguish the sign of the discriminant  $d$ .

#### 3.1. The case where the discriminant $d > 0$ .

**Theorem 3.1.** *Let  $a, b, c$  and  $g$  be integers and suppose that  $d = 4ac - b^2 > 0$ . Set  $E = \mathbb{Q}(\sqrt{-d})$ ,  $L = \mathbb{Z} + \mathbb{Z}\sqrt{-d}$  and  $H_L$  the ring class field corresponding to  $L$ . Let  $\mathbf{X} = \mathbf{Spec}(\mathbb{Z}[x, y]/(ax^2 + bxy + cy^2 + g))$ . Then  $\mathbf{X}(\mathbb{Z}) \neq \emptyset$  if and only if there exists*

$$\prod_{p \leq \infty} (x_p, y_p) \in \prod_{p \leq \infty} \mathbf{X}(\mathbb{Z}_p)$$

such that

$$\psi_{H_L/E}(\tilde{f}_E(\prod_p (x_p, y_p))) = 1$$

where  $\tilde{f}_E$  is defined the same as in (2.5) except  $F = \mathbb{Q}$ .

*Proof.* Since  $d > 0$  it is clear that  $x^2 + dy^2 = -1$  is not solvable over  $\mathbb{R}$ , which is to say the hypothesis in Proposition 2.10 holds since the only units of  $\mathbb{Z}$  are  $\{\pm 1\}$ . Then the Proposition applies, whence the result follows.  $\square$

We now give an example where the explicit criterion is obtained using this result.

**Example 3.2.** *Let  $g$  be a negative integer and  $l(x) = x^4 - x^3 + x + 1 \in \mathbb{Z}[x]$ . Write  $g = -2^{s_1} \times 7^{s_2} \times \prod_{k=1}^r p_k^{m_k}$ , where  $s_1, s_2, k \geq 0, m_k \geq 1, p_1, p_2, \dots, p_r \neq 2, 7$  are distinct primes and define*

$$D = \{p_j \mid \left(\frac{-14}{p_j}\right) = 1 \text{ and } l(x) \pmod{p_j} \text{ irreducible}\}.$$

*Then the diophantine equation  $3x^2 + 2xy + 5y^2 + g = 0$  is solvable over  $\mathbb{Z}$  if and only if*

- (1)  $g \times 2^{-s_1} \equiv \pm 1 \pmod{8}$ ,
- (2)  $\left(\frac{g \times 7^{-s_2}}{7}\right) = 1$ ,

- (3) for all  $p \nmid 2 \times 3 \times 7$ ,  $\left(\frac{-14}{p}\right) = 1$  for odd  $m := v_p(n)$ ,  
 (4) and  $\sum_{p \in D} v_p(3g) \equiv 0 \pmod{2}$ .

*Proof.* In this example, we have  $a = 3, b = 2, c = 5, d = 4ac - b^2 = 4 \times 14$ . Let  $E = \mathbb{Q}(\sqrt{-d})$ . Since  $b = 2$ , we can simplify the equation (2.2) by canceling 4 in both sides. Thus we set

$$\begin{aligned} n &= -4ag/4 = -3g, \\ \tilde{x} &= (2ax + by)/2 = 3x + y, \\ \tilde{y} &= y. \end{aligned}$$

In fact we may assume  $d = 14$  and Theorem 3.1 still applies. Because if  $d = 14$ , we still have  $E = \mathbb{Q}(\sqrt{-d})$ ,  $\tilde{x}^2 + d\tilde{y}^2 = n$  and also (2.3) holds. It follows that  $L = \mathbb{Z} + \mathbb{Z}\sqrt{-14} = \mathfrak{o}_E$  and  $H_L = H_E = E(\alpha)$  the Hilbert field of  $E$  where the minimal polynomial of  $\alpha$  is  $l(x)$ . The Galois group

$$\text{Gal}(H_L/E) = \langle \sqrt{-1} \rangle \cong \mathbb{Z}/4\mathbb{Z}.$$

Let  $\mathbf{X} = \mathbf{Spec}(\mathbb{Z}[x, y]/(3x^2 + 2xy + 5y^2 + g))$  and

$$\tilde{f}_E[(x_p, y_p)] = \begin{cases} (\tilde{x}_p + \sqrt{-14}\tilde{y}_p, \tilde{x}_p - \sqrt{-14}\tilde{y}_p) & \text{if } p \text{ splits in } E/\mathbb{Q}, \\ \tilde{x}_p - \sqrt{-14}\tilde{y}_p & \text{otherwise,} \end{cases}$$

Then by Theorem 3.1,  $\mathbf{X}(\mathbb{Z}) \neq \emptyset$  if and only if there exists

$$\prod_{p \leq \infty} (x_p, y_p) \in \prod_{p \leq \infty} \mathbf{X}(\mathbb{Z}_p)$$

such that

$$\psi_{H_L/E}(\tilde{f}_E(\prod_p (x_p, y_p))) = 1.$$

Next we calculate these conditions in details. Recall that  $n = -3g$ . By a simple calculation we know the local condition

$$\prod_{p \leq \infty} \mathbf{X}(\mathbb{Z}_p) \neq \emptyset$$

is equivalent to

$$(3.3) \quad \begin{cases} n \times 2^{-s_1} \equiv \pm 1 \pmod{8}, \\ \left(\frac{g \times 7^{-s_2}}{7}\right) = 1, \\ \text{for all } p \nmid 2 \times 3 \times 7, \left(\frac{-14}{p}\right) = 1 \text{ for odd } m, m = v_p(n). \end{cases}$$

For the Artin condition, let  $(x_p, y_p)_p \in \prod_p \mathbf{X}(\mathbb{Z}_p)$ . Then

$$(3.4) \quad (\tilde{x}_p + \sqrt{-14}\tilde{y}_p)(\tilde{x}_p - \sqrt{-14}\tilde{y}_p) = n \text{ in } E_{\mathfrak{P}} \text{ with } \mathfrak{P} \mid p.$$

And since  $H_L/E$  is unramified, for any  $p \neq \infty$  we have

$$(3.5) \quad 1 = \begin{cases} \psi_{H_L/E}(p_{\mathfrak{P}})\psi_{H_L/E}(p_{\bar{\mathfrak{P}}}), & \text{if } p = \mathfrak{P}\bar{\mathfrak{P}} \text{ splits in } E/\mathbb{Q}, \\ \psi_{H_L/E}(p_{\mathfrak{P}}), & \text{if } p = \mathfrak{P} \text{ inert in } E/\mathbb{Q}, \end{cases}$$

where  $p_{\mathfrak{P}}$  (resp.  $p_{\bar{\mathfrak{P}}}$ ) is in  $\mathbb{I}_E$  such that its  $\mathfrak{P}$  (resp.  $\bar{\mathfrak{P}}$ ) component is  $p$  and the other components are 1. We calculate  $\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)])$  separately:

- (1) If  $p = 2$ ,  $2 = \mathfrak{P}_2^2$  in  $E/\mathbb{Q}$ . Suppose  $\mathfrak{P}_2 = \pi_2 \mathfrak{o}_{E_{\mathfrak{P}_2}}$  for  $\pi_2 \in \mathfrak{o}_{E_{\mathfrak{P}_2}}$ . Noting that  $H_L/E$  is unramified, since  $\mathfrak{P}_2^2$  is principal in  $E$  but  $\mathfrak{P}_2$  is not, we have  $\psi_{H_L/E}((\pi_2)_{\mathfrak{P}_2}) = -1$ . By (3.4) we have

$$v_{\mathfrak{P}_2}(\tilde{x}_2 + \sqrt{-14}\tilde{y}_2) = v_{\mathfrak{P}_2}(\tilde{x}_2 - \sqrt{-14}\tilde{y}_2) = \frac{1}{2}v_{\mathfrak{P}_2}(n) = v_2(n) = s_1.$$

It follows that

$$\begin{aligned} \psi_{H_L/E}(\tilde{f}_E[(x_2, y_2)]) &= \psi_{H_L/E}((\tilde{x}_2 + \sqrt{-14}\tilde{y}_2)_{\mathfrak{P}_2}) \\ &= (-1)^{v_{\mathfrak{P}_2}(\tilde{x}_2 + \sqrt{-14}\tilde{y}_2)} = (-1)^{s_1}, \end{aligned}$$

where  $\tilde{f}_E[(x_2, y_2)]$  is also regarded as an element in  $\mathbb{I}_E$  such that the component above 2 is given by the value of  $\tilde{f}_E[(x_2, y_2)]$  and 1 otherwise.

- (2) If  $p = 7$ , a similar argument shows that  $\psi_{H_L/E}(\tilde{f}_E[(x_7, y_7)]) = (-1)^{s_2}$ .  
 (3) If  $(\frac{-14}{p}) = 1$  then by (3.5) we can distinguish the following cases:  
 (i)  $l(x) \bmod p$  splits into linear factors. Then  $\psi_{H_L/E}(p_{\mathfrak{P}}) = \psi_{H_L/E}(p_{\tilde{\mathfrak{P}}}) = 1$  and  $\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) = 1$ .  
 (ii)  $l(x) \bmod p$  splits into two irreducible factors. Then  $\psi_{H_L/E}(p_{\mathfrak{P}}) = \psi_{H_L/E}(p_{\tilde{\mathfrak{P}}}) = -1$ .  
 It follows that

$$\begin{aligned} \psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) &= \psi_{H_L/E}((\tilde{x}_p + \sqrt{-14}\tilde{y}_p)_{\mathfrak{P}}) \psi_{H_L/E}((\tilde{x}_p - \sqrt{-14}\tilde{y}_p)_{\tilde{\mathfrak{P}}}) \\ &= (-1)^{v_{\mathfrak{P}}(\tilde{x}_p + \sqrt{-14}\tilde{y}_p) + v_{\tilde{\mathfrak{P}}}(\tilde{x}_p - \sqrt{-14}\tilde{y}_p)} = (-1)^m, \end{aligned}$$

where  $m = v_p(n)$  since

$$\begin{aligned} v_{\mathfrak{P}}(\tilde{x}_p + \sqrt{-14}\tilde{y}_p) + v_{\tilde{\mathfrak{P}}}(\tilde{x}_p - \sqrt{-14}\tilde{y}_p) \\ = v_p(\tilde{x}_p + \sqrt{-14}\tilde{y}_p) + v_p(\tilde{x}_p - \sqrt{-14}\tilde{y}_p) = v_p(n). \end{aligned}$$

- (iii)  $l(x) \bmod p$  is irreducible. Then  $\psi_{H_L/E}(p_{\mathfrak{P}}) = -\psi_{H_L/E}(p_{\tilde{\mathfrak{P}}}) = \pm\sqrt{-1}$ . It follows that

$$\begin{aligned} \psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) &= \psi_{H_L/E}((\tilde{x}_p + \sqrt{-14}\tilde{y}_p)_{\mathfrak{P}}) \psi_{H_L/E}((\tilde{x}_p - \sqrt{-14}\tilde{y}_p)_{\tilde{\mathfrak{P}}}) \\ &= (\pm\sqrt{-1})^{v_{\mathfrak{P}}(\tilde{x}_p + \sqrt{-14}\tilde{y}_p) + v_{\tilde{\mathfrak{P}}}(\tilde{x}_p - \sqrt{-14}\tilde{y}_p)} (-1)^{v_{\tilde{\mathfrak{P}}}(\tilde{x}_p - \sqrt{-14}\tilde{y}_p)} \\ &= (\pm\sqrt{-1})^m (-1)^u \end{aligned}$$

where  $m = v_p(n)$  and  $u = v_p(\tilde{x}_p - \sqrt{-14}\tilde{y}_p)$  (in  $\mathbb{Q}_p$ ,  $0 \leq u \leq m$ ). By Hensel lemma, we can choose the local solution  $(x_p, y_p)$  suitably, such that  $u$  takes any value between 0 and  $m$ . Hence  $\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) = \pm(\sqrt{-1})^m$  with the sign chosen freely.

- (4) If  $(\frac{-14}{p}) = -1$  then  $p$  is inert in  $E/\mathbb{Q}$ . By (3.5) we have  $\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) = 1$ .  
 (5) At last if  $p = \infty$ , since  $H_L/E$  is unramified, we have  $\psi_{H_L/E}(\tilde{f}_E[(x_{\infty}, y_{\infty})]) = 1$ .

Putting the above argument together, and noting that  $D \neq \emptyset$  since  $3 \in D$  and that  $n = -3g$ , we know the Artin condition is

$$(3.6) \quad \sum_{p \in D} v_p(3g) \equiv 0 \pmod{2}.$$

The proof is done if we put the local condition (3.3) and the Artin condition (3.6) together.  $\square$



**3.2. The case where the discriminant  $d < 0$ .** In this case,  $x^2 + dy^2 = -1$  is solvable over  $\mathbb{R}$ , so we must look for other place  $p$  of  $\mathbb{Q}$  such that  $x^2 + dy^2 = -1$  is not solvable over  $\mathbb{Z}_p$ . For a rational prime  $p$  that divides  $d$ , we observe that, by Hensel Lemma,  $x^2 + dy^2 = -1$  is solvable over  $\mathbb{Z}_p$  if and only if it is solvable over  $\mathbb{Z}/p\mathbb{Z}$ , i.e.  $\left(\frac{-1}{p}\right) = 1$ . So if  $d$  is divisible by some rational prime  $p$  where  $p \equiv 3 \pmod{4}$  then  $x^2 + dy^2 = -1$  is not solvable over  $\mathbb{Z}_p$ . Otherwise if none of the prime divisors of  $d$  are congruent to 3 modulo 4, we hope that  $x^2 + dy^2 = -1$  is solvable over  $\mathbb{Z}$ , in order to make the hypothesis true in Proposition 2.10. We need the following result by Morris Newman [5].

**Theorem 3.7.** Let  $r$  be 2 or odd,  $p_1, p_2, \dots, p_r$  be distinct primes such that

$$p_i \equiv 3 \pmod{4}, \quad 1 \leq i \leq r,$$

$$\left(\frac{p_i}{p_j}\right) = -1, \quad 1 \leq i \neq j \leq r.$$

Then the diophantine equation  $x^2 - p_1 p_2 \dots p_r y^2 = -1$  has a solution.

Now we have the criterion for certain  $d < 0$ .

**Theorem 3.8.** Let  $a, b, c$  and  $g$  be integers such that  $d = 4ac - b^2 < 0$ . Suppose  $-d = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$  where  $r > 0, m_k \geq 1$  are not all even and  $p_k$  are distinct odd primes such that one of the following hypotheses holds:

- (1)  $p_i \equiv 3 \pmod{4}$  for some  $i$ .
- (2)  $r = 2$  or  $r$  is odd,  $p_i \equiv 1 \pmod{4}, m_i = 1$  for all  $i$  and  $(p_i/p_j) = -1$  for all  $i \neq j$ .

Set  $E = \mathbb{Q}(\sqrt{-d})$ ,  $L = \mathbb{Z} + \mathbb{Z}\sqrt{-d}$  and  $H_L$  the ring class field corresponding to  $L$ . Let  $\mathbf{X} = \text{Spec}(\mathbb{Z}[x, y]/(ax^2 + bxy + cy^2 + g))$ . Then  $\mathbf{X}(\mathbb{Z}) \neq \emptyset$  if and only if there exists

$$\prod_{p \leq \infty} (x_p, y_p) \in \prod_{p \leq \infty} \mathbf{X}(\mathbb{Z}_p)$$

such that

$$\psi_{H_L/E}(\tilde{f}_E(\prod_p (x_p, y_p))) = 1$$

where  $\tilde{f}_E$  is defined the same as in (2.5) except  $F = \mathbb{Q}$ .

*Proof.* The units of  $\mathbb{Z}$  are  $\{\pm 1\}$  so we only need to consider the unit  $-1$ . If (1) holds, i.e.  $p_i \equiv 3 \pmod{4}$  for some  $i$ , one can see immediately that  $x^2 + dy^2 = -1$  is not solvable over  $\mathbb{Z}_{p_i}$ . Otherwise (2) holds and then  $x^2 + dy^2 = -1$  is solvable over  $\mathbb{Z}$  by Theorem 3.7. Hence the hypothesis in Proposition 2.10 holds and we complete the proof.  $\square$

We now give an example for this case.

**Example 3.9.** Let  $g$  be a nonzero integer and  $l(x) = x^3 - x^2 - 4x + 2 \in \mathbb{Z}[x]$ . Write  $g = \pm 2^{s_1} \times 79^{s_2} \times \prod_{k=1}^r p_k^{m_k}$ , where  $s_1, s_2, k \geq 0, m_k \geq 1, p_1, p_2, \dots, p_r \neq 2, 79$  are distinct primes and define

$$D = \{p_j \mid \left(\frac{79}{p_j}\right) = 1 \text{ and } l(x) \pmod{p_j} \text{ irreducible}\}.$$

Then the diophantine equation  $5x^2 + 14xy - 6y^2 + g = 0$  is solvable over  $\mathbb{Z}$  if and only if

- (1)  $\left(\frac{g \times (-79)^{-s_2}}{79}\right) = -1$ ,
- (2) for all  $p \nmid 2 \times 5 \times 79$ ,  $\left(\frac{79}{p}\right) = 1$  for odd  $m := v_p(n)$ ,
- (3) and if  $\{p \in D \mid v_p(5g) = 1\} \neq \emptyset$  then  $r > 1$ .

*Proof.* In this example, we have  $a = 5, b = 14, c = -6, d = 4ac - b^2 = -4 \times 79$ . Let  $E = \mathbb{Q}(\sqrt{-d})$ . Since  $2 \mid b$ , we may cancel 4 in both sides and assume  $d = -79$  as we do in the previous example. And since  $79 \equiv 3 \pmod{4}$  the hypothesis (1) in Theorem 3.8 is correct. It follows that we can apply the theorem for  $d = -79$ . Thus we set

$$\begin{aligned} n &= -4ag/4 = -5g, \\ \tilde{x} &= (2ax + by)/2 = 5x + 7y, \\ \tilde{y} &= y. \end{aligned}$$

Now  $E = \mathbb{Q}(\sqrt{79})$ ,  $\tilde{x}^2 - 79\tilde{y}^2 = n$  and  $L = \mathbb{Z} + \mathbb{Z}\sqrt{79} = \mathfrak{o}_E$  and  $H_L = H_E = E(\alpha)$  the Hilbert field of  $E$  where the minimal polynomial of  $\alpha$  is  $l(x)$ . The Galois group

$$\text{Gal}(H_L/E) = \langle \omega \rangle \cong \mathbb{Z}/3\mathbb{Z}.$$

Let  $\mathbf{X} = \text{Spec}(\mathbb{Z}[x, y]/(5x^2 + 14xy - 6y^2 + g))$  and

$$\tilde{f}_E[(x_p, y_p)] = \begin{cases} (\tilde{x}_p + \sqrt{79}\tilde{y}_p, \tilde{x}_p - \sqrt{79}\tilde{y}_p) & \text{if } p \text{ splits in } E/\mathbb{Q}, \\ \tilde{x}_p - \sqrt{79}\tilde{y}_p & \text{otherwise,} \end{cases}$$

Then by Theorem 3.1,  $\mathbf{X}(\mathbb{Z}) \neq \emptyset$  if and only if there exists

$$\prod_{p \leq \infty} (x_p, y_p) \in \prod_{p \leq \infty} \mathbf{X}(\mathbb{Z}_p)$$

such that

$$\psi_{H_L/E}(\tilde{f}_E(\prod_p (x_p, y_p))) = 1.$$

By a simple computation the local condition

$$\prod_{p \leq \infty} \mathbf{X}(\mathbb{Z}_p) \neq \emptyset$$

is equivalent to the first two condition (1) and (2) above. For the Artin condition, let  $(x_p, y_p)_p \in \prod_p \mathbf{X}(\mathbb{Z}_p)$ . Then

$$(\tilde{x}_p + \sqrt{79}\tilde{y}_p)(\tilde{x}_p - \sqrt{79}\tilde{y}_p) = n \text{ in } E_{\mathfrak{P}} \text{ with } \mathfrak{P} \mid p.$$

And since  $H_L/E$  is unramified, for any  $p \neq \infty$  we have

$$(3.10) \quad 1 = \begin{cases} \psi_{H_L/E}(p_{\mathfrak{P}})\psi_{H_L/E}(p_{\bar{\mathfrak{P}}}), & \text{if } p = \mathfrak{P}\bar{\mathfrak{P}} \text{ splits in } E/\mathbb{Q}, \\ \psi_{H_L/E}(p_{\mathfrak{P}}), & \text{if } p = \mathfrak{P} \text{ inert in } E/\mathbb{Q}. \end{cases}$$

We calculate  $\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)])$  separately:

- (1) If  $p = 2$ ,  $2 = \mathfrak{P}_2^2$  in  $E/\mathbb{Q}$ . Suppose  $\mathfrak{P}_2 = \pi_2 \mathfrak{o}_{E_{\mathfrak{P}_2}}$  for  $\pi_2 \in \mathfrak{o}_{E_{\mathfrak{P}_2}}$ . Noting that  $H_L/E$  is unramified, since  $\mathfrak{P}_2$  is principal in  $E$ , we have  $\psi_{H_L/E}((\pi_2)_{\mathfrak{P}_2}) = 1$ . Hence  $\psi_{H_L/E}(\tilde{f}_E[(x_2, y_2)]) = 1$ .
- (2) If  $p = 79$ , a similar argument shows that  $\psi_{H_L/E}(\tilde{f}_E[(x_{79}, y_{79})]) = 1$ .
- (3) If  $(\frac{79}{p}) = 1$  then by (3.10) we can distinguish the following two cases:
  - (i)  $l(x) \pmod{p}$  splits into linear factors. Then  $\psi_{H_L/E}(p_{\mathfrak{P}}) = \psi_{H_L/E}(p_{\bar{\mathfrak{P}}}) = 1$  and  $\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) = 1$ .

(ii)  $l(x) \bmod p$  is irreducible. Then  $\psi_{H_L/E}(p_{\mathfrak{P}}) = (\psi_{H_L/E}(p_{\mathfrak{P}}))^{-1} = \omega^{\pm 1}$ . It follows that

$$\begin{aligned} \psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) &= \psi_{H_L/E}((\tilde{x}_p + \sqrt{79}\tilde{y}_p)_{\mathfrak{P}})\psi_{H_L/E}((\tilde{x}_p - \sqrt{79}\tilde{y}_p)_{\mathfrak{P}}) \\ &= \omega^{\pm(v_{\mathfrak{P}}(\tilde{x}_p + \sqrt{79}\tilde{y}_p) + v_{\mathfrak{P}}(\tilde{x}_p - \sqrt{79}\tilde{y}_p))} / \omega^{\pm 2v_{\mathfrak{P}}(\tilde{x}_p - \sqrt{79}\tilde{y}_p)} \\ &= \omega^{\pm(m-2u)} \end{aligned}$$

where  $m = v_p(n)$  and  $u = v_p(\tilde{x}_p - \sqrt{79}\tilde{y}_p)$  (in  $\mathbb{Q}_p$ ,  $0 \leq u \leq m$ ). By Hensel lemma, we can choose the local solution  $(x_p, y_p)$  suitably, such that  $u$  takes any value between 0 and  $m$ . Hence

$$\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) = \begin{cases} \omega^{\pm 1} & \text{if } m = 0 \text{ or } 1, \\ 1 \text{ or } \omega^{\pm 1} & \text{if } m \geq 2, \end{cases}$$

where the values are chosen freely in each case.

(4) If  $\left(\frac{79}{p}\right) = -1$  then  $p$  is inert in  $E/\mathbb{Q}$ . By (3.10) we have  $\psi_{H_L/E}(\tilde{f}_E[(x_p, y_p)]) = 1$ .

(5) At last if  $p = \infty$ , since  $H_L/E$  is unramified, we have  $\psi_{H_L/E}(\tilde{f}_E[(x_{\infty}, y_{\infty})]) = 1$ .

Putting the above argument together, and noting that  $5 \in D$  and  $n = -5g$ , we know the Artin condition is exactly the last condition (3) in the example. This completes the proof.  $\square$

#### REFERENCES

- [1] David A. Cox, *Primes of the form  $x^2 + ny^2$ : Fermat, class field theory, and complex multiplication*, John Wiley & Sons, 1989.
- [2] David Harari, *Le défaut d'approximation forte pour les groupes algébriques commutatifs*, Algebra & Number Theory **2** (2008), no. 5, 595–611.
- [3] Chang Lv and Ying Pu Deng, *On orders in number fields: Picard groups, ring class fields and applications*, Science China Mathematics **58** (2015), no. 8, 1627–1638.
- [4] J.S. Milne, *Algebraic geometry*, World Scientific Publishing Co., 1998.
- [5] Morris Newman, *A note on an equation related to the pell equation*, American Mathematical Monthly (1977), 365–366.
- [6] Dasheng Wei, *On the sum of two integral squares in quadratic fields  $\mathbb{Q}(\sqrt{\pm p})$* , Acta Arith. **147** (2011), no. 3, 253–260.
- [7] ———, *On the Diophantine equation  $x^2 - Dy^2 = n$* , Science China Mathematics **56** (2013), no. 2, 227–238.
- [8] ———, *On the sum of two integral squares in the imaginary quadratic field  $\mathbb{Q}(\sqrt{-2p})$* , Science China Mathematics **57** (2014), no. 1, 49–60.
- [9] Dasheng Wei and Fei Xu, *Integral points for multi-norm tori*, Proceedings of the London Mathematical Society **104** (2012), no. 5, 1019–1044.
- [10] ———, *Integral points for groups of multiplicative type*, Advances in Mathematics **232** (2013), no. 1, 36–56.

SKLOIS, INSTITUTE OF INFORMATION ENGINEERING, CAS, BEIJING 100093, CHINA  
E-mail address: lvchang@amss.ac.cn